Is it possible to use the device on more than one computer to access Internet Banking?

Yes. It just requires an initial installation to take place and then you will be able to plug it into any computer that has been set up. And the good news is that the Internet CFO® Cash Manager 'cookie' will be placed on the device, so it will travel with you. Landmark Bank does not recommend using this device or conducting financial transactions from any public access computer such as at a library or hotel or with Wi-Fi access.

Are there any fees for the IronKey Trusted Access solution?

Yes. We are offering this solution at a nominal fee. Contact us for more information.

What happens if the IronKey Trusted Access device is lost or stolen?

Immediately call Landmark Bank at (800) 618-5503. Depending on the situation, we will either disable or detonate the lost/stolen device and replace it with a new one, if required. Please note that if we replace the lost or stolen device, there is a device replacement cost that will apply.

Landmark Bank
here for you.

LandmarkBank.com

(800) 618-5503

MEMBER FDIC

EQUAL HOUSING LENDER

IronKey®

Trusted Access for Banking

Landmark Bank

Landmark Bank has partnered with IronKey®, an Internet security company, to offer the "Trusted Access" solution to our business customers conducting ACH origination for payroll or payments, wire transfers, or online bill payments via our Internet Banking "Internet CFO®" service. Trusted Access is a secure USB plug-in device that is designed to create a clean and secure tunnel connection to Internet Banking to help prevent man-in-the-browser, man-in-the-middle, and key logging attacks.

The online criminal world has increased their efforts of targeting small-to-medium sized businesses. Why? Because criminals know that if they can hit just one business, they can steal much more in assets versus an individual. With little technical support and limited budgets, many medium to small businesses are now being targeted because of lapses in their security.

"Hackers" are criminals that use malicious software known as malware to secretly access and take partial or complete control of a computer without the owner's consent. A computer can become unknowingly infected by malware which has been embedded from software downloads, email attachments (links, documents, images), a compromised website, or application exploits (i.e. flaws in a Web browser, media player [video or music], instant-messaging client, or social networking sites [links, downloads, videos, photos, documents]). This malware can then spread across a business' internal network to other workstations or laptops.

Once installed, the malware provides the information that enables the cyber thieves to impersonate the business in online banking sessions. The hackers use the information to log into the businesses Internet Banking account where they have access to and can review the account details including account activity and patterns related to ACH and wire transfer origination parameters (such as file size and frequency limits). Now the perpetrators are able to initiate illegal wire transfers and/or ACH transactions. Conducted this way, these unauthorized transactions appear to the bank as legitimately conducted by the company or employee.

Funds withdrawn from one of these accounts are typically routed to banks in the U.S. and credited to accounts recently opened by the criminals or their unwitting accomplices (called "mule accounts") for the express purpose of receiving and laundering these funds. The funds are promptly withdrawn or wired overseas, making recovery extremely difficult. This type of crime is known as "corporate account take over."

Landmark Bank recommends customers take special precautions to protect their computers and business by establishing best practices such as: educating everyone in your company about this type of threat; enhancing the security of computer systems and networks; limiting computer use such as email and Internet surfing; establishing account controls with dual authorizations and transaction dollar limits; creating strong passwords and changing them a few times per year; and reconciling all banking transactions on a daily basis. Immediately escalate any suspicious transactions to us. There is a limited recovery window for these fraudulent transactions and reacting quickly may prevent further loss.

We work hard to protect your information on this end to ward off any threats, but now we believe it's time to take the next step in protecting your accounts. Landmark Bank is here to work with you to help defend your business from cyber-threats which is why we are offering the Trusted Access security device. While no technology is 100% fail proof, this security solution is designed to prevent criminals from stealing personal information and it meets the FFIEC, FBI, and NACHA guidelines for safe online banking without a difficult installation. Providing an additional level of security to our customers is very important to us.

Trusted Access by IronKey
Frequently Asked Questions

What is the IronKey Trusted Access solution?

IronKey Trusted Access provides a safer environment for conducting online business banking by utilizing a portable USB security device to store a tamper-proof virtual environment that runs completely separate of other applications on a computer.

How does the IronKey Trusted Access device work?

By plugging the device into the USB drive of the computer, the Trusted Access application invokes its own operating system and secure Internet browser, along with encrypting both the keyboard and information being displayed on the screen. While we cannot promise any technology to be 100% fail proof, this combination of security layers is designed to prevent criminals from stealing personal information. Think of Trusted Access as a standalone secured computer running side-by-side the host computer.

Are there system requirements for Trusted Access to work?

Yes. The minimum system requirements are:

- **Operating systems:** Windows XP, Vista, or 7 (32 and 64 bit versions)
- **Minimum of 2 GB RAM** required
- **Network Connection –** wireless and DSL may slow down the device performance (dial-up may not work at all)
- **Local Administrator rights are required** during the initial driver installation only
- **USB 2.0** (high-speed) port
- Trusted Access **will not work in remote access sessions** such as PC Anywhere, Remote Desktop Connection, VPN connection, or Log-Me-In.